УДК 004.4
**Т. Яцюк**
(Тернопільський державний технічний університет імені Івана Пулюя)

## VHDL-модель базових операцій на еліптичних кривих

Особливий інтерес до криптографії еліптичних кривих (ЕК) обумовлений такими перевагами – швидкодія та невелика довжина ключа. Однак для забезпечення повного ефекту цих переваг необхідні спеціальні алгоритми і засоби для швидкої роботи алгоритму і генерації стійких до атак параметрів. Усі криптосистеми захисту інформації реалізовані апаратно, програмно або так і так. Будь-який криптографічний алгоритм може бути реалізований у вигляді деякої програми. Переваги такої реалізації очевидні:

- програмні засоби шифрування легко копіюються;
- вони прості у використанні;
- їх неважко модифікувати відповідно до конкретних потреб.

В усіх розповсюджених операційних системах засоби шифрування файлів є вбудованими. Звичайно вони призначені для шифрування окремих файлів, і робота з ключами цілком покладається на користувача або на певний алгоритм. Тому застосування цих засобів вимагає особливої уваги: по-перше, ні в якому разі не можна зберігати ключі на диску разом із зашифрованими з їх допомогою файлами, а по-друге, незашифровані копії файлів необхідно стерти відразу ж після шифрування.

Багато засобів криптографічного захисту даних реалізовано у виді спеціалізованих апаратних пристроїв. Ці пристрої вбудовуються в лінію зв’язку і здійснюють шифрування всієї переданої по ній інформації. Перевага апаратного шифрування над програмним обумовлено декількома причинами .

По-перше, апаратне шифрування має більшу швидкість. Криптографічні алгоритми складаються з величезного числа складних операцій, виконуваних над бітами відкритого тексту. Сучасні універсальні комп’ютери погано пристосовані для ефективного виконання цих операцій. Спеціалізоване устаткування вміє робити їх набагато швидше.

По-друге, апаратуру легше фізично захистити від проникнення ззовні тому, що ж вона зазвичай міститься в особливих контейнерах, що унеможливлює зміну схеми її функціонування.

І по-третє, апаратура шифрування більш проста в установці. Дуже часте шифрування потрібно там, де додаткове комп’ютерне устаткування є зовсім зайвим. Телефони, факсимільні апарати і модеми значно дешевше обладнати пристроями апаратного шифрування, чим вбудовувати в них мікрокомп’ютери з відповідним програмним забезпеченням.

Навіть у комп’ютерах установка спеціалізованого шифрувального устаткування створює менше проблем, чим модернізація системного програмного забезпечення з метою додавання в нього функцій шифрування даних. В ідеалі шифрування повинне здійснюватися непомітно для користувача, тому за допомогою сучасних систем автоматизованого проектування, таких як Active-HDL, Quartus, Synplicity, можна спроектувати компоненти, що реалізують базову операцію криптоалгоритмів на основі еліптичних кривих, додавання двох точок в кінцевих полях, та основну операцію – скалярне множення в кінцевих полях.

Результатами проведених розробок є VHDL моделі компонент та проведена їх імплементація на мікросхеми сімейства FLEX10K від фірми Altera. Використання розроблених компонент в подальшому проектуванні криптосистем на основі еліптичної криптографії дозволить розробити повноцінну криптосистему, яка неодмінно буде часто використовувати реалізовані базові операції на ЕК.